BIOMETRIC IDENTIFICATION SYSTEM USING BIOMETRIC IMAGES AND COPY PROTECT CODE STORED ON A MAGNETIC STRIPE AND ASSOCIATED METHODS

Related Applications

This application is based upon prior filed copending provisional applications No. 60/271,300 filed February 23, 2001, No. 60/279,466 filed March 28, 2001, No. 60/281,265 filed April 3, 2001, No. 60/293,113 filed May 23, 2001, and No. 60/334,656 filed October 31, 2001 the entire disclosures of which are incorporated herein by reference.

Field of the Invention

The present invention relates to the field of biometric identification and verification, and, more particularly to biometric verification using a card with biometric image data and a copy protect code stored thereon.

Background of the Invention

Biometric verification and identification may be desirable for a number of business applications. For example, biometric verification at a point-of-sale terminal offers the possibility to reduce credit card fraud. A biometric characteristic of the purchaser can be compared with a biometric characteristic

stored on the credit card. If there is a match, the transaction is authorized.

U.S. Patent No. 5,432,864 to Lu et al. discloses a biometric verification approach wherein track 3 of a magnetic stripe on a credit card can be used to store so-called "Eigenface parameters". The Eigenface parameters may be reduced to less than 100 bytes according to the patent. Unfortunately, the Eigenface parameters may not be sufficiently accurate in confirming the card bearer's identify.

Along those lines, U.S. Patent No. 5,355,411 to MacDonald discloses storing on magnetic tracks, an electronic signature and user's portrait. U.S. Patent No. 4,752,676 to Leonard et al. discloses comparing voice print information with stored data on a magnetic stripe. Again, such characteristics may not provide a sufficiently high accuracy rate to be practically used.

U.S. Patent No. 4,995,086 to Lilley et al. discloses magnetic tracks on a plastic card that store fingerprint related data. The stored data is for a degree of correlation between a fingerprint of the authorized individual and a stored and selected reference signal image and the code number of this reference signal image. A fingerprint detection terminal with a sensor contains a memory win which the selected reference signal image is stored. The sensor compares the actual fingerprint of an individual to be checked with the corresponding reference signal image identified on the plastic card and stored in the fingerprint detection terminal. The determined degree of correlation is compared to

the degree of correlation stored on the plastic card to determine if the person bearing the card is the authorized user. Unfortunately, the approach disclosed is fairly complicated and may lead to inaccuracy in terms of false acceptance and/or false rejection rates.

Summary of the Invention

In view of the foregoing background, it is therefore an object of the invention to provide a reliable and accurate biometric identification and verification system and methods.

This and other objects, features and advantages in accordance with the present invention are provided by a method for storing biometric information on a token having a magnetic storage medium. The method includes capturing a biometric image and generating biometric data therefrom. Further, the method includes generating a copy protect code, and storing the biometric data and the copy protect code on the magnetic storage medium of the token.

The biometric information is preferably based upon a fingerprint while capturing the biometric image comprises capturing the biometric image using a fingerprint sensor. The copy protect code may be encrypted. The token preferably comprises a card corresponding to the ANSI/ISO/IEC 7810 standard and the magnetic storage medium comprises a magnetic stripe having three tracks in accordance with the ANSI/ISO/IEC 7810 standard. Here, storing the biometric data and copy protect code includes storing the biometric data and copy protect code on the third

track of the magnetic stripe. Also, generating the copy protect code includes combining at least some of the data stored on first and second tracks of the magnetic stripe.

The array of image pixels may include a series of consecutive and colinear image pixels. The token may comprise a generally rectangular substrate, and may be an access card, credit card, debit card, identification card or smart card.

Another aspect of the present invention is directed to a method of regulating the use of a token, the token comprising at least one of an access card, credit card, debit card, identification card and smart card, and including at least a magnetic storage medium thereon. The method includes enrolling an authorized token user by capturing a first biometric image and generating therefrom first digital pixel data for a first array of image pixels, processing the first digital pixel data to produce enrollment biometric data, generating a copy protect code, and storing the enrollment biometric data and copy protect code on the magnetic storage medium of the token. Furthermore, the method includes verifying an identity of a token holder presenting the token by capturing a second biometric image and generating therefrom second digital pixel data for a second array of image pixels, processing the second digital pixel data to produce verification biometric data, verifying the copy protect code stored on the magnetic medium, and comparing the verification biometric data with the enrollment biometric data stored on the magnetic storage medium of the token to

determine if the token holder is the authorized token user.

A system aspect of the invention includes a system for regulating the use of a token, the token comprising at least one of an access card, credit card, debit card, identification card and smart card, and including at least a magnetic storage medium thereon. The system includes an authorized token user enrollment unit including a first biometric sensor device for capturing a first biometric image and generating therefrom first digital pixel data for a first array of image pixels, a first image processor for processing the first digital pixel data to produce enrollment biometric data, a copy protect code generator for generating a copy protect code, and a first magnetic storage medium reader/writer for writing the enrollment biometric data and the copy protect code on the magnetic storage medium of the token. Also, the system includes at least one token holder verification unit for verifying the identity of a token holder presenting the token, and comprising a second biometric sensor device for capturing a second biometric image and generating therefrom second digital pixel data for a second array of image pixels, a second image processor for processing the second digital pixel data to produce verification biometric data, a second magnetic storage medium reader for reading the enrollment biometric data and the copy protect code from the magnetic storage medium of the token, a copy protect code verification unit for verifying the copy protect code, and a comparator for comparing the verification

biometric data produced by the second image processor with the enrollment biometric data stored on the magnetic storage medium of the token to determine if the token holder is the authorized token user.

Each of the biometric sensor devices preferably comprises a fingerprint sensor, and may include a finger slide, finger guides and a finger stop. Also, the token may comprise a card corresponding to the ANSI/ISO/IEC 7810 standard and the magnetic storage medium comprises a magnetic stripe having three tracks in accordance with the ANSI/ISO/IEC 7810 standard. Here, the first magnetic storage medium reader/writer writes the enrollment biometric data and copy protect code on the third track of the magnetic stripe.

The copy protect code generator may comprise a longitudinal redundancy check (LRC) character calculator for calculating an LRC character based upon a combination of data stored on first and second tracks of the magnetic stripe. Here, the copy protect code verification unit preferably comprises a second LRC calculator for calculating a second LRC character based upon a combination of data stored on first and second tracks of the magnetic stripe to generate a verification copy protect code, and a code comparator for comparing the copy protect code stored on the third track of the magnetic stripe with the verification copy protect code.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of an enrollment unit of the biometric identification and verification system in accordance with the present invention.

FIG. 2 is a schematic diagram of a verification unit of the biometric identification and verification system in accordance with the present invention.

FIG. 3 is a schematic diagram of a card including a magnetic stripe in accordance with the present invention.

FIG. 4 is a schematic diagram of a sensing device in accordance with the enrollment and verification units of FIGs. 1 and 2.

FIG. 5 is a schematic diagram of the sensor of sensing device of FIG. 4.

FIG. 6 is a flowchart illustrating the steps of the biometric identification and verification method in accordance with the present invention.

FIG. 7 and 8 are schematic diagrams of the software architecture for implementing the method and system of the present invention.

FIG. 9 is an embodiment of a Device Configuration Table.

FIG. 10 is an embodiment of an Encoding Approach Table.

FIG. 11 is a table illustrating an embodiment of the Standard Biometric Template of the software architecture of FIGs. 7 and 8.

FIG. 12 is a table illustrating an embodiment of the Algorithm Biometric Template of the software architecture of FIGs. 7 and 8.

FIG. 13 is a table illustrating and Error Bit Rate Increment Counter.

FIG. 14 is a table illustrating an embodiment of the Standard Digitized Array of Image Pixels of the software architecture of FIGs. 7 and 8.

Detailed Description of the Preferred Embodiments

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

As will be appreciated by those skilled in the art, portions of the present invention may be embodied as a method, data processing system, or computer program product. Accordingly, these portions of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment combining software and hardware aspects. Furthermore, portions of the present invention may be a computer program product on a computer-usable storage medium having computer readable program code on the medium. Any suitable computer readable medium may be utilized including, but not limited to, static and dynamic storage

devices, hard disks, optical storage devices, and magnetic storage devices.

The present invention is described below with reference to flowchart illustrations of methods, systems, and computer program products according to an embodiment of the invention. It will be understood that blocks of the illustrations, and combinations of blocks in the illustrations, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, implement the functions specified in the block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory result in an article of manufacture including instructions which implement the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide

steps for implementing the functions specified in the flowchart block or blocks.

Referring to FIGs. 1-4, a system for regulating the use of a token 30 will now be described. The token 30 (FIG. 3) includes a substrate 32 and a magnetic storage medium 34, such as a magnetic stripe, thereon. The system includes an authorized token user enrollment unit 10 (FIG. 1) including a first biometric sensor device 12 for capturing a first biometric image and generating therefrom first digital pixel data for a first array of image pixels. An image processor 14 selects a first plurality of spaced apart sets of image pixels from the first array of image pixels, and processes respective sets of digital pixel data for the first plurality of selected spaced apart sets of image pixels to produce enrollment biometric data. A magnetic storage medium reader/writer 16 writes the enrollment biometric data on the magnetic storage medium 34 of the token 30.

Furthermore, the system includes at least one token holder verification unit 20 (FIG. 2) for verifying the identity of a token holder presenting the token 30. For example, the token holder is typically the owner of the card. The unit 20 also has a biometric sensor device 22 for capturing a second biometric image and generating therefrom second digital pixel data for a second array of image pixels. A second magnetic storage medium reader 26 reads the enrollment biometric data from the magnetic storage medium 34 of the token 30, and a comparator 24 compares the second digital pixel data with the enrollment

biometric data stored on the magnetic storage medium 34 of the token 30 to determine if the token holder is the authorized token user.

The biometric sensor device 22 is preferably a biometric sensor 44 having a sensing area 70 while the plurality of spaced apart sets of image pixels comprises a reference set of image pixels based upon a predetermined location, such as a centerline C (FIG. 5), on the sensing area, and at least one other set of image pixels a predetermined distance from the reference set or centerline. The biometric sensor devices 12, 22 may each comprise an image quality determination unit 18, 28 for determining the quality of captured biometric images. Each set of image pixels may comprise a series of consecutive and colinear image pixels.

The biometric information is preferably based upon a fingerprint while the biometric sensor devices each comprise a fingerprint sensor 44. The biometric sensor device may further comprise a finger slide 42 adjacent the fingerprint sensor 44. Also, the finger slide 42 may have finger guides 46 and a finger stop 48. Again, the magnetic storage medium preferably includes a magnetic stripe 34 having three tracks in accordance with the ISO/IEC 7810 and 7811 standards, while the magnetic storage medium reader/writer preferably writes the enrollment biometric data on the third track.

It will be appreciated that the embodiment described above enrolls a fingerprint image and subsequently compares another fingerprint image for verification. Much as described in U.S. Patent No.

6,075,876 to Dragonoff, which is herein incorporated by reference in it's entirety, the enrollment extracts yardsticks, or a set of image pixels, which may comprise half-lines, whole lines, or columns. The yardsticks are preferably of uniform size, and each yardstick preferably contains black-white data for the image to be enrolled. Preferably the enrollment stores data in a suitable format. When comparing an image to be verified, in a simple case (for line art), the first yardstick is compared with the acquired image (which preferably is larger than the enrollment window). It will be understood that electronic signals or data for "images" are compared, rather than optical images themselves, in the preferred embodiment. In the preferred algorithm, the first (stored) yardstick is sought to be matched with a given line of the acquired image, and is compared on a bit-by-bit basis. Absent finding a match, the yardstick is shifted along the line, or, if necessary, will shift to another line, and seek a match along that row. Assuming a match results for the first yardstick, other spaced apart yardsticks are next compared to the image to be verified, and can be shifted left or right a limited amount, or not at all, depending on skew. If the best match is below a tolerance, verification is positive. This technique may also be applied also to grey scale data.

It should also be appreciated that while the preferred embodiments herein refer to a magnetic medium such as a magnetic stripe on a card, nothing precludes the method and system from storing the information on any other type of storage medium, such

as, but not limited to, dynamic memories, e.g. optical and magneto-optical, and/or static memories, e.g. semiconductor or integrated circuit memories.

A method for storing biometric information on a token having a magnetic storage medium will be described with reference to FIG. 6. The method includes capturing a biometric image 102 and generating therefrom digital pixel data for an array of image pixels, and, at 106, selecting a plurality of spaced apart sets of image pixels from the array of image pixels. Also, the method includes processing respective sets of digital pixel data for the selected spaced apart sets of image pixels to produce biometric data 108, and storing the biometric data on the magnetic storage medium of the token 110.

As discussed above, capturing the biometric image may include using a biometric sensor 44 having a sensing area 70, and selecting the plurality of spaced apart sets of image pixels may include selecting a reference set of image pixels based upon a predetermined location on the sensing area, such as the centerline C, and selecting at least one other set of image pixels a predetermined distance from the reference set. The location of the reference set of image pixels and the other set(s) of image pixels may also be stored on the magnetic storage medium. Capturing the biometric image may include capturing multiple biometric images until a preferred biometric image is captured based upon a resolution threshold as indicated by the quality check block 104.

Again, each set of image pixels may be a series of consecutive and colinear image pixels. Also, the

biometric information is preferably based upon a fingerprint while capturing the biometric image may include capturing the biometric image using a fingerprint sensor. The token 30 (FIG. 3) preferably comprises a card 32 corresponding to the ISO/IEC 7810 standard and the magnetic storage medium comprises a magnetic stripe 34 having three tracks in accordance with the ISO/IEC 7811 standard. Here, storing the biometric data preferably includes storing the biometric data on the third track. The token 30 may be a generally rectangular substrate such as an access card, credit card, debit card, frequent flyer card, driver's license card, identification card and/or smart card.

The method may further include verifying an identity of a token holder presenting the token by capturing a second biometric image 112 and generating therefrom second digital pixel data for a second array of image pixels, decoding the biometric data stored on the magnetic storage medium 116 and comparing the second digital pixel data with the first plurality of selected spaced apart sets of image pixels of enrollment biometric data stored on the magnetic storage medium of the token to determine if the token holder is the authorized token user 118. Again, the quality of the image may be checked 114.

Further, the method may include generating a copy protect code, and storing the copy protect code on the magnetic storage medium of the token 122, and/or obtaining a personal identification number (PIN), and storing the PIN on the magnetic storage

medium of the token 124. Verifying the PIN stored on the magnetic medium may include reading the PIN from the magnetic storage medium, requesting a verification PIN from the token holder (block 126), and comparing the PIN read from the magnetic storage medium with the verification PIN (block 130). Also, the copy protect code may be encrypted, and generating the copy protect code may include combining bits of data stored on the magnetic stripe. Generating the copy protect code, may, for example, include calculating a longitudinal redundancy check (LRC) character based upon a combination of data stored on first and second tracks of the magnetic stripe. Of course, the verification process would include verifying the copy protect code stored on the magnetic medium 128.

A more specific embodiment of the method and system for reliable and accurate biometric identification and verification will be described with reference to FIGs. 7 and 8. The following describes the encoding system and process that is used for biometric enrollment. Biometric enrollment is the process that is followed to capture and encode a biometric or an individual's unique physical characteristic (fingerprint, eye, hand, face, etc.) on a magnetic stripe of an identification or smart card. By encoding a biometric on a credit, debit, ATM, Frequent Flyer, Driver's License or other identification or smart cards, the secured identification card can be used to authorize credit, debit, check cashing, cash withdrawals, wire transfer and other financial transactions; to identify card

holders at security checkpoints and to provide positive identification. This embodiment describes the encoding of fingerprint image pixels on a magnetic stripe of an Identification or Smart Card but the system could be successfully used for encoding other biometric characteristics.

The Card Encoding Module 224 prompts the user to "Swipe the card" and initiates the Standard Interface Module 232 to read the magnetic stripe. For enrollment, the user is prompted to place their fingers on a finger slide 42 and moves their fingers forward. The finger slide 42 (Figure 4) controls the positioning of the finger over the sensor 44 and is used to minimize the finger placement rotation and skew on the sensor. As the finger is slid into position, the finger slide has a stop 48 that restricts any further forward movement into the finger slide over the sensor. The finger guides/wedges 46 separate the fingers in such a way as to minimize the rotation or "roll" of the finger on the sensor.

This embodiment of the encoding/decoding system hardware includes a fingerprint sensor module 12, microcontroller 14, 24, serial ports 58 and 60, LCD display 50, user switches 52, power supply, power switch 54, power connector 56, case 62, magnetic card reader/writer 16, and magnetic card reader 26. The microcontroller oversees all internal system functions including the fingerprint sensor, LCD display, and user switches. Control of the external RS-232 serial ports is also managed by the microcontroller. The external serial ports

facilitate communication with the magnetic card reader/writer and optional connection to a host or PC. The on-board power supply includes voltage regulators and power management circuitry to ensure reliable operation over a wide range of supply voltages and temperatures.

A biometric device such as a fingerprint sensor 202 provides signals representing image pixels. There are many types of fingerprint sensors. Each type of sensor may utilize different technologies to capture the fingerprint image. Optical based sensors use cameras and lens to capture the image. Capacitive sensors utilize a silicon integrated circuit containing an array of capacitive sensor plates. Each sensor plate produces a capacitance measurement whose value becomes a gray-scale value that becomes part of the image. Recently, new technology- based sensors have been introduced in the marketplace. For example, some new sensors are able to generate a small AC electric field between the integrated circuit and the fingers "live" layer. Elements in the sensor receive the signals and create digital patterns that mimic very accurately the fingerprint structure. The operational characteristics of each fingerprint sensor vary widely by manufacturer and the use of technology in terms of clarity, resolution and accuracy of the image. Sensors that use the AC electric field technology appears to provide a more accurate and clearer image than those captured by other technologies since the new sensors are capable of detecting the ridges and valleys in the "live" layer

of cells that are located below the surface of the skin.

The Sensor Processing Module 206 is responsible for selecting and creating a good array of image pixels. The fingerprint sensor 202 captures the image and uses an Analog to Digital Converter to digitize the array of image pixels. The following process is followed to insure a good array of fingerprint image pixels is available in the Algorithm Biometric Template 216 for processing. If a good image cannot be provided, another array of image pixels is requested from the fingerprint sensor.

The fingerprint sensor histogram is used to determine if the fingerprint image is of good clarity by analyzing the pixel distribution across the histogram. The image is enhanced by power and phase adjustments. The fingerprint sensor 202 using an A/D converter generates a digitized grayscale array of image pixels. The Module 206 checks for correct centering of the finger within the grayscale array of image pixels. The black/white balance within the grayscale array of image pixels is checked to insure that the image is not too dark or light. The Module 206 counts ridges in the center of the grayscale array of image pixels to determine if the image is of good clarity. The ridge count is verified to be between the minimum and maximum ridge tolerances. The number of consecutive gap widths of one pixel in length is measured to insure that there is not an excessive level of noise in the image.

The encoding system 200 utilizes the Enrollment Algorithm Module 214 to analyze the digitized array

of image pixels to select several "yardsticks" or a plurality of spaced apart sets of image pixels that are the most effective for biometric identification to be encoded onto a Magnetic Stripe of an Identification or Smart Card. After the centerlines of the array of image pixels are selected, the first "yardstick" is identified based upon selecting one of two sets of image pixels that are located at a predetermined plus or minus equivalent distance from either the horizontal or vertical centerline. At least one other "yardstick" is identified based upon selecting one of two sets of image pixels that are located at another predetermined plus or minus equivalent distance from either the horizontal, vertical or diagonal centerline.

The sets of image pixels are selected and stored in the algorithm biometric template 216 by analyzing each "yardstick" according to the following process: The number of ridges are counted; The maximum gap between the ridges are measured to determine if any fingerprint scars or scrapes exist; The variance between the ridge count and minimum and maximum ridge thresholds are determined; The set of image pixels with the smallest maximum gap is identified; and The yardsticks with sets of image pixels with the smallest ridge variance and smallest maximum gap between the ridges are selected based upon the "best fit" method.

After a good enrollment is achieved and if the "Hard to Enroll" was not depressed, the enrollment must be verified as will be discussed in further detail below. If more than one verification fails,

the "Enrollment is Unsuccessful" and a new enrollment may be attempted using another finger.

The Card Encoding Module 224 supports various encoding approaches which would be defined in an Encoding Approach Table, as would be readily appreciated by the skilled artisan. The encoding approach is established at "compile time" in the Device Configuration Table (FIG. 9) after analyzing the requirements of the magnetic stripe of the identification or smart card including the track number to be encoded, maximum size of the "algorithm biometric template", maximum characters per track, data format and track format.

The Card Encoding Module 224 creates a header that is included in standard biometric template 230 to identify the Software Version Number (FIG. 11). The Software Version Number may relate to the Enrollment/Verification Algorithm Modules 214, 218, Card Encoding/Decoding Module 224, 228 and/or an Encoding Approach Number. The Card Encoding Module 224 prompts the user to enter their Personal Identification Number (PIN) from "000" to "999" using the switches for entering the 100's, 10's and 1's digits of the number (Figure 4; 52). As the PIN is entered, the number will be displayed on the LCD screen 50. After the user completes entering the PIN, the "Enter" switch is depressed. The encoding system encrypts the PIN and includes it the standard biometric template 230.

If the "Hard to Enroll" Flag switch is depressed, the Card Encoding Module 224 prompts the user to enter their Extended Personal Identification

Number (PIN) from "0" to "9" using the switch for entering the 1's digits of the number. Again, as the PIN is entered, the number will be displayed on the LCD screen. After the user completes entering the Extended PIN, the "Enter" switch is depressed. The encoding system encrypts the Extended PIN and includes it in the standard biometric template 230.

The Card Encoding Module 224 creates a Copy Protect Code from the data on the magnetic stripe. The code is encrypted and included in the standard biometric template 230. The copy protect code is preferably determined by combining bits of data on the two tracks that are not being written on. The Copy Protect Code is six bits, the seven bit code, less the parity bit, for example. The Copy Protect Code is used to prevent track data from being altered or biometric image pixels from being copied from one Magnetic Stripe on an Identification or Smart Card to a Magnetic Stripe on another Identification or Smart Card.

Beginning with the bit in the upper, left-most corner of the algorithm biometric template 216, 226 (FIG. 12), the Card Encoding Module 224 translates the bits left to right, top to bottom four, five or six bits at a time into the standard biometric template 230 (FIG. 11). Using the encoding approach number identified in the Device Configuration Table (FIG. 9), an Encoding Translation Table is selected from Column 6 of the Encoding Approach Table (FIG. 10).

Note: All of the Encoding Approach Numbers (0 - 10) in FIG. 10 can be encoded on Track 2 but would

not comply with the ISO or AAMVA track format standards. Some Magnetic Stripe Card Readers/Writers will read and write 86 characters on a track in the AAMVA format. Some Magnetic Stripe Card Readers/Writers support a "Custom" mode in which ANSI/ISO control characters are not recognized. The track density is 210 bits per inch (bpi) unless otherwise specified.

Using the Encoding Translation Table, four, five or six bits as identified in Column 1 are translated to either a ANSI/ISO alphanumeric or numeric character data format. The ANSI/ISO hex data format may also be indicated. No translation is required for "Custom" track formats.

The Card Encoding Module 224 analyzes the four, five or six bits translated at a time in the standard biometric template 230 to determine if they are control, reserved or other characters that require a special translation. Depending upon the magnetic stripe or smart card reader/writer, the control, reserved or other characters that require special translation may be translated to one or two ANSI/ISO alphanumeric or numeric characters. The Card Encoding Module 224 analyzes the four, five or six bits translated at a time in the standard biometric template 230 to determine if the bits can be compressed with succeeding sequences bits. The bits may be compressed using several standard compression algorithms to reduce the size of the biometric template. The bits may be encrypted using a standard encryption algorithm.

The Card Encoding Module 224 prompts the Enroll Finger Code to be entered from "0" to "7" using the

switches for entering the 1's digits of the number. As the Enroll Finger Code is entered, the number will be displayed on the LCD screen 50. After the user completes entering the Enroll Finger Code, the "Enter" switch is depressed. The encoding system encrypts the Enroll Finger Code and includes it in the standard biometric template 230. The Enrollment Finger Code will be used to prompt the user to place the proper finger on the sensor during Verification. If the size of the standard biometric template 230 exceeds the maximum number of characters per track as defined in the Encoding Approach Table (FIG. 10: column 4) for the selected encoding approach , a new image is selected and the enrollment process is performed again.

The Card Encoding Module 224 sets the Error Bit Rate Increment Counter in the standard biometric template 230 to reflect that a PIN was entered. The Error Bit Rate Increment Counter will be added to the base Error Bit Rate to improve the likelihood of a successful verification. If the "Hard to Enroll" switch was depressed, the Card Encoding Module 224 sets the Error Bit Rate Increment Counter (FIG. 13) in the standard biometric template 230 to reflect that an Extended PIN was entered.

The Magnetic Stripe or Smart Card Reader/Writer Module 234, 238 encodes the standard biometric template 230 on the magnetic stripe of identification or smart cards using a magnetic stripe or Smart card reader/writer 236, 240 according to the coercivity code in the Device Configuration Table.

After a successful write to the magnetic stripe, the "Enrollment is Successful" message is displayed.

The following describes the decoding system and process that is used for biometric verification. Biometric verification is the process that is followed to decode a biometric or an individual's unique physical characteristic (fingerprint, eye, hand, face, etc.) from a magnetic stripe of an identification or smart card. By verifying a biometric on a credit, debit, ATM, Frequent Flyer, Driver's License or other identification or smart cards, the "secured identification card can be used to authorize credit, debit, check cashing, cash withdrawals, wire transfer and other financial transactions; to identify card holders at security checkpoints and to provide positive identification. This embodiment describes the decoding of fingerprint image pixels on a magnetic stripe of an Identification or Smart Card but the system could be successfully used for decoding other biometric characteristics.

The Magnetic Stripe or Smart Card Reader/Writer Module 234, 238 decodes the standard biometric template 230 from the magnetic stripe of a identification or smart cards using a Magnetic Stripe or Smart card Reader/Writer Module 236, 240. The Software Version Number information in the Header of the standard biometric template is used to determine which Verification Algorithm Module 218, Card Decoding Module 228 and Encoding Approach Number will be used in the decoding process. The Card Decoding Module 228 analyzes the bits in the standard

biometric template 230 to determine if they are compressed. If required, the bits are decompressed using a decompression algorithm. The Card Decoding Module 228 analyzes the bits in the standard biometric template 230 to determine if they are encrypted. If required, the bits are decrypted using a decryption algorithm.

Using the Encoding Translation Table that was used during Enrollment, the Card Decoding Module 228 software searches the standard biometric template 230 to determine if one or two ANSI/ISO alphanumeric or numeric characters as defined in the Encoding Translation Table can be found. If a match occurs, the one or two control, reserved or other characters are translated to the ANSI/ISO alphanumeric or numeric character. Using the Encoding Translation Table that was used during Enrollment, the Card Decoding Module 228 translates either the ANSI/ISO alphanumeric or numeric character in the standard biometric template 230 to four, five or six bits at a time.

The Card Decoding Module 228 decrypts the "Code" in the standard biometric template 230 and compares it to the Copy Protect Code that is determined by combining at least some of the data on the two tracks that do not contain "biometric template" data on the swiped identification card. If the Copy Protect Codes do not match, a "Copy Protect Code Violation" message is displayed on the LCD screen 50 and the Verification process is discontinued.

The Card Decoding Module 228 decodes the Personal Identification Number (PIN) in the standard

biometric template 230. The user is asked to enter their PIN "000" to "999" using the switches 52 for entering the 100's, 10's and 1's digits of the number. As the PIN is entered, the number will be displayed on the LCD screen. After the user completes entering the PIN, the "Enter" switch is depressed.

If the "Hard to Enroll" flag is set, the Card Encoding Module software decodes the Extended PIN in the standard biometric template 230. The user is prompted enter their Extended Personal Identification Number (PIN) from "0" to "9" using the switch for entering the 1's digits of the number. As the PIN is entered, the number will be displayed on the LCD screen. After the user completes entering the PIN, the "Enter" switch is depressed.

For verification, the user is prompted on the LCD screen to place the correct finger (using the Enrolled Finger Code) on a finger slide 42 and to move their fingers forward. Again, the finger slide controls the positioning of the finger over the fingerprint sensor and is used to minimize the inconsistency of placement of the finger on the sensor for each placement attempt.

The Sensor Processing Module 206 is responsible for selecting and creating a good image. If a good image cannot be provided, another image is requested from the fingerprint sensor 202. The following process is followed to insure a good image or array of image pixels are available in the Algorithm Biometric Template 216 for processing. The fingerprint sensor histogram is used to determine if

the fingerprint image is of good clarity by analyzing the pixel distribution across the histogram. The image is enhanced by power and phase adjustments. The fingerprint sensor using an A/D converter generates a digitized grayscale array of image pixels. The Module 206 checks for correct centering of the finger within the grayscale array of image pixels. The black/white balance within the grayscale array of image pixels is checked to insure that the image is not too dark or light. The Module 206 counts ridges in the center of the grayscale array of image pixels to determine if the image is of good clarity. The ridge count is verified to be between the minimum and maximum ridge tolerances. The number of consecutive gap widths of one pixel in length is measured to insure that there is not an excessive level of noise in the image. To minimize false rejections, an Error Bit Increment Counter (FIG. 13) in the Standard Biometric Template 230 will be added to the base Error Bit Rate.

The Verification Algorithm Module 218 takes the First "yardstick" in the standard biometric template 230 retrieved from the Magnetic Stripe of an Identification or Smart Card and makes a comparison to those yardsticks in the Algorithm Biometric Template 216. In the Algorithm Biometric Template 216, the bit by bit comparison begins at the lowest horizontal or vertical scanline and incrementally continues to the highest horizontal or vertical scanline. The bits in the scanline are shifted until the bits begin to match. A match is found if after the comparison of a scanline is completed, the number of bits that don't match are less than the First

Yardstick Error Bit Rate. If no match is found, the array of image pixels are rotated 1 pixel to adjust for image rotation and skew and the match is repeated. If no match is found after the array of image pixels are rotated a maximum number of times as defined by a Rotation Threshold, another biometric image is captured by the fingerprint sensor 202 and another search is performed if a system "timeout" did not occur. If a system timeout occurs, "Verification is Unsuccessful" is displayed on the screen 50.

If a match to the First "yardstick" is successful, the Verification Algorithm Module 218 takes the remaining "yardsticks" in the "standard biometric template" 230 and makes a comparison to those in the Algorithm Biometric Template 216. Using the First Other Yardstick offset location in the trailer record, the offset is added to the First Yardstick location and a bit by bit match is performed in the scanline. If the number of bits that don't match which are added to the First Other Yardstick Error Counter are less than the First Other Error Bit Rate, a match for the second Other Yardstick is performed. Using the Second Other Yardstick offset location in the trailer record, the offset is added to the First Yardstick location and a bit by bit match is performed in the scanline. If the number of bits that don't match in the Second Other Yardstick Error Counter are greater than Second Other Error Bit Rate, the First Other Yardstick search process begins again from the First Yardstick location plus or minus one scanline to accommodate the stretching of the skin. If no match exists for

First Other Yardstick, another biometric image is captured by the fingerprint sensor 202 and another First Yardstick search is performed if a system "timeout" did not occur. If a system timeout occurs, "Verification is Unsuccessful" is displayed on the screen 50.

After the First and Second Other Yardsticks are found, the (Third thru "N") Other Yardstick searches process begins by adding the (Third thru "N") Other Yardstick offset locations in the trailer record to the First Yardstick location. If the accumulated count of errors in the (Third thru "N") Other Yardstick Error Counter is greater than the (Third thru "N") Error Bit Rate after all the "yardsticks" in the standard biometric template 230 are compared, the verification is unsuccessful. For unsuccessful verifications, another biometric image is captured by the fingerprint sensor 202 and another search is performed if a system "timeout" did not occur. If a system timeout occurs, "Verification is Unsuccessful" is displayed on the screen 50.

If the accumulated count of errors in the (Third thru "N") Other Yardstick Error Counter is less than the (Third thru "N") Error Bit Rate after all the "yardsticks" in the "standard biometric template" are compared and no PIN or Extended PIN match errors occurred, "Verification is Successful" on the LCD screen. An authorization code and other data may be also transmitted to a host computer. If the count of errors in the verification counter is greater than the Error Bit Rate after all the "yardsticks" in the standard biometric template are compared or a PIN or

Extended PIN error occurred, "Verification is Unsuccessful" is displayed on the LCD screen.

To insure that all tracks are not copied from the magnetic stripe of one card to another, information such as the cardholder's name and credit card number are displayed on the LCD 50. The displayed information can be used to validate the information on the transaction source documents to insure that they are the same following a "Successful Verification".

The architecture of the encoding/decoding image pixel software is designed and structured to allow new biometric sensors, enrollment algorithms, verification algorithms, magnetic stripe readers/writers and smart card readers/writers to be easily substituted for the components that are described in this embodiment. For example, a new fingerprint sensor 202 can be substituted for the existing sensor by connecting the new sensor to the device and installing a new Sensor Processing Module 206. No other changes would be required to the encoding/decoding computing system hardware or software to support the new sensor.

Sensor Processing Module 206 Functions: Acquires a good array of image pixels -Assures the image meets the minimum clarity threshold requirements; Converts the Sensor Array of Image Pixels 204 to Standard Digitized Array of Image Pixels 210 (FIG. 14); Processes the following Standard Application Program Interface Module 220 sensor commands: Calibrate - to calibrate the biometric sensor 202, Reset - to reset the biometric sensor, Image - to acquire the image of

the finger that was last enrolled or verified, Status - to display the current status of the sensor or sensor commands.

Sensor Interface Module 208 Functions: Using the Device Configuration Table (FIG. 9), initiates the Sensor Processing Module 206 -Sensor Processing Module is determined at "compile time", -Sensor Baud Rate is determined at "compile time"; and Initiates all the sensor 202 commands.

Enrollment Algorithm Module 214 Functions: Processes Enroll command -Initiates the Sensor Interface Module; Basic functions: establishes the centerline of the image, Determines best first "yardstick" and location, Determines best other "yardsticks" and locations; If Successful Enrollment -Creates Algorithm Biometric Template, and -Returns to Card Encoding Module via Standard API Module; If Unsuccessful Enrollment -If possible, selects another Enrollment Algorithm Module 214 using Device Configuration Table, and -If not possible, prompts user "Enrollment is Unsuccessful."

Verification Algorithm Module 218 Functions: Processes Verify command -Initiate the Sensor Interface Module; Basic functions -Starts search for First "Yardstick" in the Standard Biometric Template 230, -After the First "Yardstick" is found, search for the Other "Yardsticks" at the location stored in Standard Biometric Template 230, -If "Verification is Successful", Prompt user "Verification is Successful" and display the cardholders name and number, -If Unsuccessful Enrollment, Prompt user "Verification is Unsuccessful."

Control and Standard Application Program Interface Module 220 Functions (API): During program initialization, -Prompts the user to enter the nine numeric character Device Control Code using the LCD, compare the entered Device Control Code to the code in the Device Configuration Table, if the Device Control Code is not, discontinue the operation, -Sets the coercivity in the magnetic card reader/writer to the default according to the Device Configuration Table, -Configure reader/writer for "ISO plus AAMVA"; If the "Enroll" switch is depressed, initiates the Card Encoding Module using the Device Configuration Table; If the "Verify" switch is depressed, initiates the Card Decoding Module using the Device Configuration Table; If the "Calibrate" switch is depressed, processes the command using the Sensor Processing Module; If the "Reset" switches are depressed, processes the command to reset the Fingerprint Sensor Module 202, Microcontroller, LCD display and Magnetic Stripe Reader/Writer 236, 240; If the "Coercivity" switch is depressed, processes the command and updates the coercivity field in the Device Configuration Table; If the "Hard to Enroll" switch is depressed, processes the command, sets the Hard to Enroll Code in Standard Biometric Template 230 and initiates the Card Encoding Module 224 using the Device Configuration Table; Processes the "Status" and "Image" commands by initiating the Sensor Processing Module 206; Process Upload/download commands, Upload and download of Algorithm Biometric Template 216; Switch use: Switch 1 & 4 - "Reset", Switch (left) - "Coercivity" and 100's number entry,

Switch 2 - "Hard to Enroll" and 10's number entry, Switch 3 - "Enroll" and (0 to 9) number entry and "Yes" entry, Switch 4 (right) - "Verify" and "Enter" and "No" entry, and Switch 2 & 3 - "Calibrate."

Card Encoding Module 224: Prompts user communication via LCD Display to "Swipe Card"; Initiates read of card using Standard Magnetic Card Interface Module 232; Prompts user to "Place finger on Sensor" ; Initiates the Enrollment Algorithm Module 214 using Device Configuration Table; If enrollment is good, initiates the Verification Algorithm Module 218 four times to verify enroll is good, -If all four verifies are not good, prompt user "Enrollment is Unsuccessful", -Each Verify does not require a card swipe; Selects encoding approach from Device Configuration Table; Adds Header to Standard Biometric Template 230; Requests enter of PIN, encodes and adds to Standard Biometric Template 230, -To minimize false rejections, sets the Error Bit Rate Increment Counter in Standard Biometric Template 230 to standard value if PIN is entered; If Hard to Enroll Flag is set, requests enter of Extended PIN, encodes and adds to Standard Biometric Template 230, -To minimize false rejections, sets the Error Bit Rate Increment Counter in Standard Biometric Template 230 to standard value if Extended PIN is entered; Creates Copy Protect Code, encodes and adds to Standard Biometric Template 230; Using Encoding Approach Number in Device Configuration Table, selects Encoding Translation Table and translates Algorithm Biometric Template 216 data into Standard Biometric Template 230; Using Encoding Approach

Number in Device Configuration Table, use Encoding Translation Table and translates control, reserve and other characters in Standard Biometric Template 230; Compresses data, if necessary, in Standard Biometric Template 230; Encrypts data in Standard Biometric Template 230; Check for maximum length of Standard Biometric Template 230; Initiates the write of the Standard Biometric Template 230 to the magnetic stripe using the Standard Magnetic Card Interface Module 232; and Prompts user that "Enrollment is Successful."

Card Decoding Module: Prompts user communication via LED Display to "Swipe Card"; Initiates Read of card into Standard Biometric Template using the Standard Magnetic Card Interface Module; Using the header, determine the Enrollment/Verification Algorithm module 214, 218 and Card Encoding/Decoding module 224, 228 to be used; Verify modules are available in software by using device control table; Tests for fingerprint data on card; If no fingerprint data, prompt user that "No Enrollment Information on Card"; If biometric template data is encrypted, decrypt the data, if required; If biometric template data is compressed, de-compress data, if required; Using Encoding Approach Number in Header and Device Configuration Table, translates control, reserve and other characters in Standard Biometric Template 230; Using Encoding Approach Number in Header and Device Configuration Table, translates all chacters in the Standard Biometric Template 230; De-codes and verify Copy Protect Code in Standard Biometric Template 230, -If Copy Protect Code is not valid, Prompts user:

"Invalid Copy Protect Code"; Requests enter of PIN; If the Hard to Enroll flag is set, requests enter of Extended PIN; Stores Header, yardstick and trailer in the Algorithm Biometric Template 216; Using the Enroll Finger Code, prompts user to "Place finger on Sensor" and initiates Verification Algorithm Module 218 using the Standard API Module 220.

Standard Magnetic Card Interface Module 232: Initiates the Read into the Standard Biometric Template 230, -Use the Device Configuration Table to determine Card Reader/Writer Module 234, 238 to initiate; Initiates the Write from the Standard Biometric Template 230, -Use the Device Configuration Table to determine Card Reader/Writer Module 234, 238 to initiate.

Card Reader/Writer Module 234, 238: Card Reader Module, -Using the Encoding Approach Table and Device Configuration Table, reads the card data into the Standard Biometric Template 230 from the Magnetic Stripe or Smart Card Reader/Writer 236, 240; Card Writer Module, -Using the Encoding Approach Table and Device Configuration Table, writes the card data from the Standard Biometric Template 230 to the Magnetic Stripe or Smart Card Reader/Writer 236, 240.

Encoding/decoding computing system hardware: A preferred embodiment of the Fingerprint Sensor Module includes a Motorola 56309 Digital Signal Processor (DSP), AuthenTec AF-S2 "FingerLoc" fingerprint sensor with analog to digital converter, Serial port for connection to microcontroller, and a Parallel port; LCD display having a 2 lines by 20 characters/line display; a Jackrabbit RCM2020

microcontroller with Serial port connection to Fingerprint Sensor Module (9600 bps), Serial port connection to a Magnetic Stripe Card Reader/Writer (9600 bps), Serial port for future connection to a host or PC (9600 bps), Parallel port or another connection to LCD display, Four switches, and One Reset switch; Magnetic Stripe Card Reader/Writer, e.g. a AMC C722; Circuit Board with Power supply, Power connections and Serial connections.

The disclosures of related applications entitled "BIOMETRIC IDENTIFICATION SYSTEM USING A MAGNETIC STRIPE AND ASSOCIATED METHODS" (atty. Docket No. 59718); and "BIOMETRIC IDENTIFICATION SYSTEM USING BIOMETRIC IMAGES AND PERSONAL IDENTIFICATION NUMBER STORED ON A MAGNETIC STRIPE AND ASSOCIATED METHODS" (atty. Docket No. 59731) to the same inventor and concurrently filed herewith are incorporated by reference herein in their entirety.

Many modifications and other embodiments of the invention will come to the mind of one skilled in the art having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is understood that the invention is not to be limited to the specific embodiments disclosed, and that modifications and embodiments are intended to be included within the scope of the appended claims.